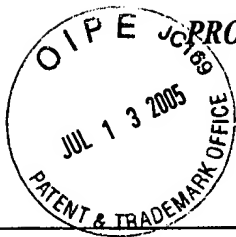


19/20/99
15 U.S. PTO



PROVISIONAL APPLICATION FOR PATENT
COVER SHEET

Case No. WHOVIS.018PR

Date: September 20, 1999

Page 1

JCS53 U.S. PTO
60/154734
09/20/99

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: PROVISIONAL PATENT APPLICATION

Sir:

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR § 1.53(c).

For: **SECURE SITE FOR INTERNET TRANSACTIONS**

Name of First Inventor: Alexander Dickinson
Residence Address: Laguna, California

Name of Second Inventor: Robert Dobson
Residence Address: 15 Inverary, Dove Canyon, CA 92679

Name of Third Inventor: Brian Berger
Residence Address: 23518 Sandstone, Mission Viejo, CA 92692

Name of Fourth Inventor: Adriaan Ligtenberg
Residence Address: 735 Holly Oak Drive, Palo Alto, CA 94303

Enclosed are:

- (X) Specification in 23 pages.
- (X) 2 sheets of drawings.
- (X) A check in the amount of \$150 to cover the filing fee is enclosed.
- (X) A return prepaid postcard.
- (X) The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Was this invention made by an agency of the United States Government or under a contract with an agency of the United States Government?

(X) No.

() Yes. The name of the U.S. Government agency and the Government contract number are:

**PROVISIONAL APPLICATION FOR PATENT
COVER SHEET**

Case No. WHOVIS.018PR

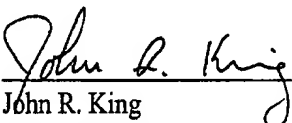
Date: September 20, 1999

Page 2

(X) Please send correspondence to:

John R. King
Knobbe, Martens, Olson & Bear, LLP
620 Newport Center Dr., 16th Floor
Newport Beach, CA 92660

Respectfully submitted,



John R. King
Registration No. 34,362

G:\DOCS\VRK\VRK-2296.DOC:sb
092099

KNOBBE, MARTENS, OLSON & BEAR

A LIMITED LIABILITY PARTNERSHIP INCLUDING
PROFESSIONAL CORPORATIONS

PATENT, TRADEMARK AND COPYRIGHT CAUSES

620 NEWPORT CENTER DRIVE

SIXTEENTH FLOOR

NEWPORT BEACH, CALIFORNIA 92660-8016

(949) 760-0404

FAX (949) 760-9502

INTERNET WWW.KNOB.COM

RICHARD E CAMPBELL
MARK M ABUMERI
JON W. GURKA
KATHERINE W WHITE
ERIC M NELSON
ALEXANDER C CHEN
MARK R BENEDICT
PAUL N CONOVER
ROBERT J ROBY
SABING H LEE
KAROLINE A DELANEY
JOHN W HOLCOMB
JAMES J MULLEN, III
JOSEPH S CIANFRANI
JOSEPH M REISMAN
WILLIAM R ZIMMERMAN
GLEN L NUTTALL
ERIC S FURMAN
DO TE KIM
TIRZAH ABE LOWE
GEOFFREY Y IIDA
ALEXANDER S FRANCO
SANJIVPAL S GILL
SUSAN M MOSS
GUY PERRY
JAMES W HILL, M.D.
ROSE M THIESSEN
MICHAEL L FULLER
GINGER R DREGER

OF COUNSEL
JERRY R SEILER

JAPANESE PATENT ATTY
KATSUHIRO ARAI**

EUROPEAN PATENT ATTY
MARTIN HELLEBRANDT

KOREAN PATENT ATTY
MINCHEOL KIM

SCIENTISTS & ENGINEERS
(NON-LAWYERS)

RAIMOND J SALENIEKS**
NEIL S BARTFELD**
DANIEL E JOHNSON**
JEFFERY KOEPKE
KHURRAM RAHMAN
JENNIFER A HAYNES
BRENDAN P O NEILL
MARRINA Q MEI
THOMAS Y. NAGATA
ALAN C. GORDON
PABLO S HUERTA
LINDA H LIU
MICHAEL J HOLIHAN
YASHWANT N VAISHNAV

LOUIS J. KNOBBE*
DON W. MARTENS*
GORDON H. OLSON**
JAMES B. BEAR
DARRELL L. OLSON*
WILLIAM B. BUNKER
WILLIAM H. NIEMAN
LOWELL ANDERSON
ARTHUR S. ROSE*
JAMES F. LESNIAK
NED A. ISRAELSEN
DREW S. HAMILTON
JERRY T. SEWELL
JOHN B. SGANGA, JR.
EDWARD A. SCHLATTER
GERARD VON HOFFMANN
JOSEPH R. RE
CATHERINE J. HOLLAND
JOHN M. CARSON
KAREN VOGEL WEIL*
ANDREW H. SIMPSON
JEFFREY L. VAN HOOSEAR
DANIEL E. ALTMAN
ERNEST A. BEUTLER
MARGUERITE L. GUNN
STEPHEN C. JENSEN
VITO A. CANUSO III
WILLIAM H. SHREVE
LYNDA J. ZADRA-SYMES**

STEVEN J. NATAUPSKY
PAUL A. STEWART
JOSEPH F. JENNINGS
CRAIG S. SUMMERS
ANNEMARIE KAISER
BRENTON R. BABCOCK*
THOMAS F. SMEGAL, JR.
MICHAEL M. TRENNHOLM
DIANE M. REED
JONATHAN A. BARNEY
RONALD J. SCHOENBAUM
JOHN R. KING
FREDERICK S. BERRETTA
NANCY WAYS VENSKO
JOHN P. GIEZENTANNER
ADEL S. AKHTAR
THOMAS R. ARNO
DAVID N. WEISS
DANIEL HART
JAMES T. HAGLER
DOUGLAS G. MUEHLHAUSER
LORI LEE YAMATO
STEPHEN M. LOBBIN
ROBERT F. GAZDZINSKI
STACEY R. HALPERN*
MICHAEL K. FRIEDLAND
DALE C. HUNT
LEE W. HENDERSON
DEBORAH S. SHEPHERD

Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Attorney Docket No. : WHOVIS.018PR

Applicants : Dickinson, et al.

For : SECURE SITE FOR INTERNET
TRANSACTIONS

Attorney : John R. King

"Express Mail"

Mailing Label No. : EL 417 342 053 US

Date of Deposit : September 20, 1999

I hereby certify that the accompanying

Transmittal in Duplicate; Specification in pages; sheets of drawings;
Check for Filing Fee; Return Prepaid Postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Donald L. King

G:\DOCS\VRK\VRK-2297.DOC

SECURE SITE FOR INTERNET TRANSACTIONSBackground of the Invention5 Field of the Invention

The invention relates to a system and method of using a biometric sensor to provide secure access to an Internet site. More particularly, the invention relates to a method of providing secure Internet transactions using biometric data.

Description of the Related Art

10 A commonly available means for identifying computer users is the use of passwords. More recently, biometric mechanisms such as fingerprint sensors are available that allow for extremely reliable identification of users. However, few compelling applications have been proposed for the use of such devices in network environments. Existing examples of such applications include: OS logon, client/file
15 encryption, and access to Internet/WEB sites.

Cryptography generally relies on the user possessing and keeping secret a cryptographic key. Such a key may be used to digitally sign or encrypt a document. Previously this secrecy has been implemented by having the user keep the key in the user's physical possession. Such possession has typically taken the form of keeping the
20 key on the hard disk of the user's computer or more securely on a "Smart" or "Chip" card. Such means of maintaining secrecy has a number of weaknesses. In particular, a hard disk is typically an insecure environment in which the key may be fraudulently copied. Even Smart cards are typically protected only by a four-digit pin. More generally, giving responsibility to the user for protecting the most critical part of the
25 system, is not an intuitively secure solution.

Summary of the Invention

One aspect of the invention relates to an alternative scheme that does not rely on the user's ability to protect the secret key in any way. In this scheme the private key is stored within an ultra secure server (USS) and associated with a biometric template
30 unique to the owner of the private key. The USS is configured to meet the following requirements:

1. Under absolutely no conditions may the private key leave the USS.

2. The private key must only be accessed upon presentation of an incoming biometric template that matches the stored template.

3. Upon matching, the private key may be only used to enable a limited set of standard cryptographic operations such as digital signatures and encryption.

Another aspect of the invention involves a secure (WEB) site that includes a secure server and the USS which is associated with the secure server. The secure site is maintained by a service provider which allows each registered and enrolled user to access a user-specific site that provides links to user-selected Internet services.

Brief Description of the Drawings

Figure 1 shows a first embodiment of a communications system.

Figure 2 shows a second embodiment of a communications system.

Detailed Description of the Preferred Embodiment

Figure 1 shows an overview of a communications system in which several computers (PC) and one or more online vendors OV have access to the Internet. A biometric (fingerprint) sensor is connected to each computer and each computer is assigned to a user U1, U2. The system includes further a secure site which can be accessed by the users U1, U2 and the online vendors OV.

The computers provide for hardware or software encryption of the users' fingerprints. In one embodiment, a WEB browser provides for the encryption and communication occurs via a conventional Internet protocol IP.

The secure site is formed by a secure server SS in combination with an ultra secure server USS. The USS includes a biometric match processor, an encryption processor, and a secure memory. The secure memory comprises pairs of biometric templates and private keys. The USS communicates with the SS via a SCSI bus. In one embodiment the secure memory may be a large bank of smart cards each containing the biometric template, private key and a cryptographic engine. In such a configuration, neither the biometric or secret key would need to leave the confines of the smart card.

During an enrollment procedure, the fingerprint (template) of a new user is obtained and stored in the secure memory. This fingerprint template is then available in the secure site to allow the new user subsequent access to the secure site.

The security of the transmission of the biometric template is protected. Two means are listed as follows:

1. At the point of acquisition of the biometric template (e.g., the Biometric sensor) the template is encrypted with the public key of the secure server. This insures that only the secure server that is in possession of the matching private key may encrypt the template.

2. At the point of acquisition of the biometric template (e.g., the Biometric sensor) the template is encrypted with the public key of the user. This insures that the template may only be decrypted given access to the users private key, which is stored at the secure server SS. This scheme insures that even if the server's private key is compromised, the biometric templates will remain secure.

The invention involves several applications for the secured site. Such applications include, for example, providing secure email or documents, secure Web pages, secure (Internet) chat, trusted e-commerce portals, and public key-pair generation. The invention involves three inter-related concepts: the use of a "Secure Hot Key," a trusted community and a trusted e-commerce portal.

The Secure Hot Key activity takes place when a biometric sensor is attached to a network access device such as PC, PDA or Cellular phone. User activation of the device, such as (a user touching fingerprint sensors) initiates the following sequence.

1. The user's identity is verified by matching the new biometric sample to a previously stored sample held on the client or dedicated network server.

2. Once identified, the server provides the user access to a secure set of services. Such access may for example be provided as a WEB page provided by the server that includes Web links that represent such services.

Trusted Community:

Given the existence of the above-described "secure hot key," identity of users accessing the server can be determined with a high degree of certainty. Creation of such a "Trusted Community" enables the provisions of a number of unique services for members of the community. The services include (with reference to Figure 1):

Secure and trusted Email or document:

All senders and receivers of email have absolute confidence that the sender of an email or recipient of an email are of unambiguous identity.

(1) U1 creates a document on the secured server SS and adds a digital signature to the created document using the fingerprint sensor and the ultra secure server USS.

(2) U2 receives the signed document in his account on the SS.

(3) U2 uses his fingerprint and the USS to

(a) decrypt the received document with his private key

(b) create a digitally signed receipt that is returned to U1 for tracking.

That is U1 can monitor if U2 receives and opens the document.

(4) Note: Either U1 or U2 may be part of the network. For example, if U2 is not part of the network both U1 and U2 can send and receive documents, however, the guaranteed tracking function will not work.

Secure Web pages, trusted Web:

For instance for medical documents and e-commerce services.

(1) U1 creates a Web page and signs it with a digital signature using the biometric sensor and the USS.

(2) U2 views the Web page and uses the USS to decrypt the page and digitally sign a receipt that is sent to U1.

Secure and trusted chat:

For instance for doctor/patient discussions.

(1) U1 creates a line of text and uses the USS to encrypt and sign the line of text.

(2) U2 uses the USS to decrypt the line of text and creates a receipt for U1.

Trusted E-Commerce Portal

In addition to services outlined above that involve peer to peer interactions within the community additional user services can be created as the community communicates with external entities such as other WEB sites. The general purpose of

such communications is expected to be the provision of electronic commerce services to members of the community.

(1) U1 is authenticated using the USS.

(2) The SS contacts the online vendor OV and assures the OV as to U1's identity.

(3) The SS may generate a session key and distribute it to U1 and OV so that they may have a secure transaction.

Public key-pair generation:

(1) Pairs of private and public keys can be created inside the USS.

(2) The private key is stored in the secure memory.

(3) The public key is put into a digital certificate data structure and is published.

However, an annotation is made in the certificate to the effect that the corresponding private key is biometrically protected. This permits the receiver of a signed document to verify the biometric signing.

With reference to Figure 2, the trusted community can be used as a "trusted firewall" between the user and the merchant. Because the community has reliable information as to the user's identity, it can extract certain user properties such as the user's ability to pay and carry these properties to the merchant. In this situation, after the user has selected items for purchase at the merchant's WEB site, the community can clear payment for goods and services without ever revealing the identity of the user. This arrangement benefits both the user whose privacy is preserved and the merchant who is assured payment. Note that, whereas, the link between user and community is made using biometric identification means, the links between the community and merchants may use standard cryptographic techniques as the later links are between secure computer servers not individuals. In this mode, the community as acting as the trusted portal between the user and the merchants.

Payment methods include at least two novel mechanisms for clearing payments from the community to a merchant using the existing credit card infrastructure.

1. At the time of payment the portal generates a one-time use credit card number and informs the credit card company of this number and the expected amount of the transaction. The portal then provides this number of the merchant who uses normal credit card validation techniques to ensure payment to the merchant.

5 2. Credit card companies issue card members with a card whose members with a card whose number is not valid for normal Internet transactions. That is to say, when this card number is provided directly to an Internet merchant, any attempted clearance of the transactions will fail. The only exception to this failure, occurs if the merchant notifies the card company during the verification process that the number was
10 received over a link from the trusted portal. This arrangement allows credit card holders to shop using their card in non-Internet environments as usual but protects against theft of that number and subsequent fraudulent use on the Internet.

WHAT IS CLAIMED IS:

1. An apparatus for a secure network site, comprising
 - a first processor configured to match a biometric data of a present user with stored biometric data of registered users;
 - 5 a memory associated with the first processor, the memory storing at least one of a private key and biometric data of a registered user; and
 - a second processor associated with the memory and the first processor and configured to encrypt data.

10

G:\DOCS\MOH\MOH1681.DOC:cc
091699

6600250 "42454.053

The Problem

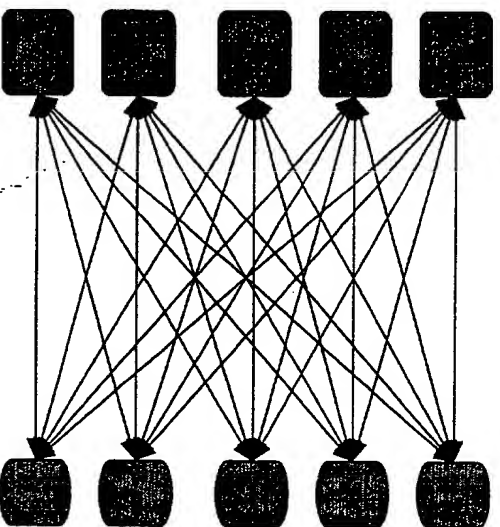
- At present, Web customers and vendors must establish trust each time a new commercial relationship is being established:
 - Customer asks "do I trust this vendor to send me the product and protect my payment information?"
 - Vendor asks "do I trust this customer to pay?"
- With the explosive growth in both number of vendors and potential customers, this is a key factor slowing down the adoption of c-to-b and b-to-b e-commerce

The Solution

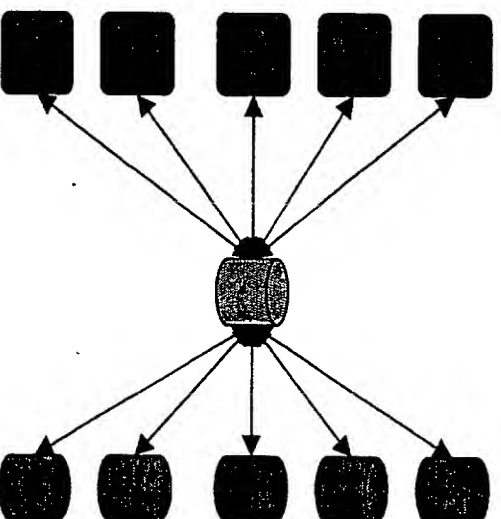
- Through the creation of a trusted portal we can massively reduce the number of trusted relationships:
 - Customer establishes trust once with the portal
 - Vendor establishes trust once with the portal
 - The portal assures the customer that privacy is maintained with any vendor
 - The portal assures the vendor that payment will be made with any customer

The Solution (2)

**1-to-1:
Many trust relationships**



**Trusted Portal:
Far fewer trust relationships**



Customers



Vendors



Trusted Portal

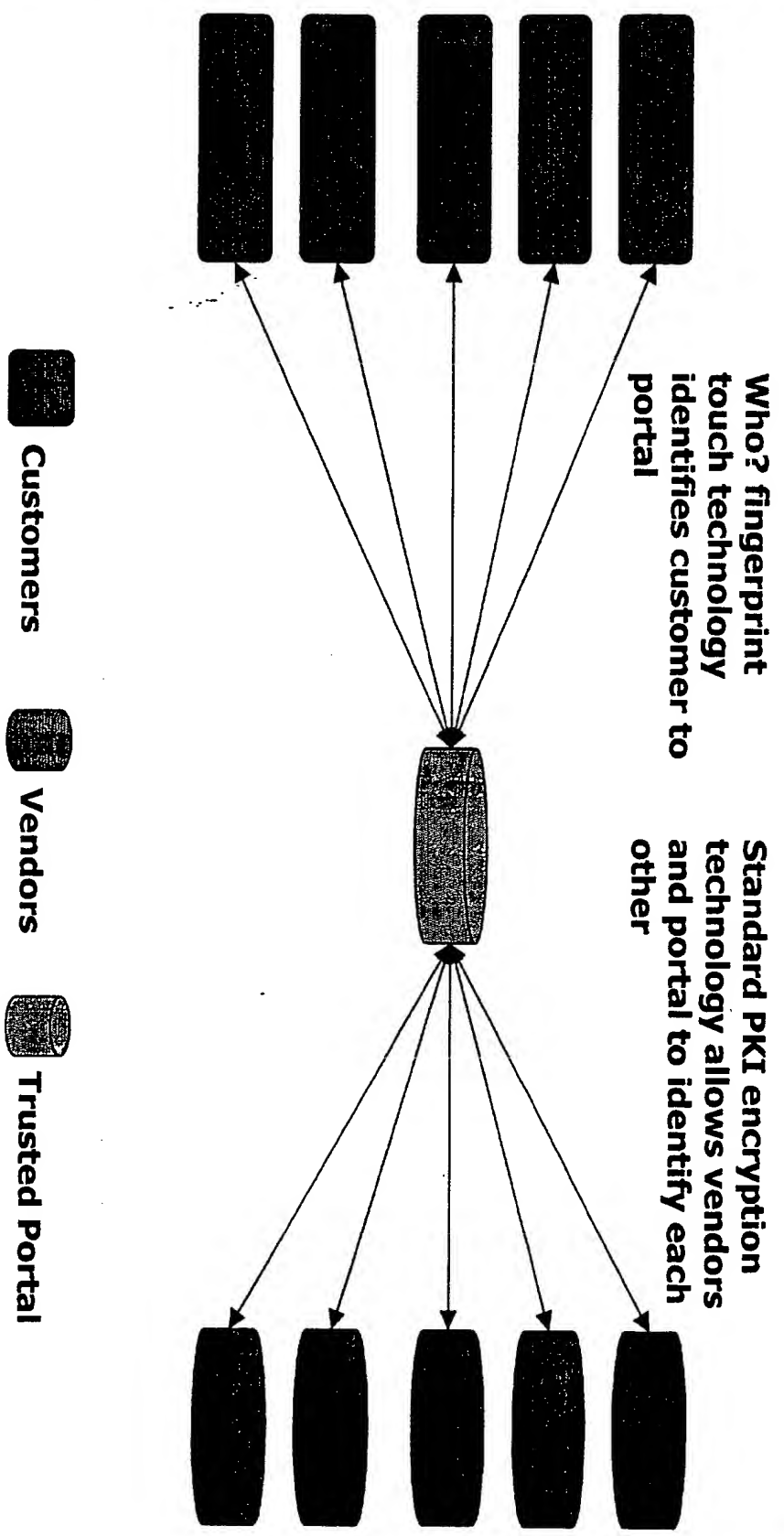
How does it work?

- One touch on a finger sensor takes the customer to the trusted portal - a private, customized page is displayed to which only that customer has access
- From that page, the customer can jump to any qualified vendor site and carry out a transaction simply and without any privacy concerns
- As the trusted portal hands the customer over to the vendor, the portal promises the vendor that it will handle payment

How is this possible?

- Existing in-place software technology (digital certificates, public key encryption, virtual private networks) make it easy for one server to identify another - so the trusted portal can be sure of the vendor's identity and visa-versa
- However these technologies fail when it comes to identifying people, not machines
- By using a single fingerprint touch to enter the trusted portal, we can be assured of the identity of the person and create a non-repudiable event

Operation



Enormous Potential

- A trusted portal will generate extraordinary revenue opportunities:
 - The elimination of identity fraud will reduce costs for both vendors and payment players (credit card co's, banks) - a portion of these savings can be turned to revenue
 - Real-time data on customers buying behavior can be used for targeted advertising: banner ads, sales, coupons etc.
 - Achieving critical mass will open opportunities for lower credit card costs and "click-through" payments from vendors
 - Other value-added services may be created such as "child-safe" chat rooms and trusted-site search engines

Strategy: Building a web community

- Why do we want a community?
- ! **Network economics:** value proposition grows with the number of members - creates huge entry barriers (e.g. ebay)
- ! **Value:** once in the community, members can be sold an increasing diversity of services (e.g. VerticalNet)
- ! **Adoption & growth:** community members must communicate with each other: early adopters will buy multiple nodes, followers will only need a single node to communicate with the installed base (e.g. the exponential growth of fax machine market)

How do I get there?

- One touch on a finger sensor at any location takes the user into the trusted community - it appears as a personalized web page that only the user can access
- Once the user has entered the community, he or she can participate in diverse B2B services

What do I do there?

- Send and receive totally secure encrypted email
- Send, receive and gain receipt of secure documents (e.g. legal documents usually sent by FedEx)
- Create and access secure web sites (e.g. small company proprietary business data)
- Participate in secure e-commerce (e.g. complete a mortgage transaction entirely on-line)
- Access chat rooms with secured membership (e.g. doctor/patient dialogs)

How does it work?

- The community is built on a full-fledge public key security system: items are digitally signed and encrypted using standards-based PKI
- Its unique feature is that the user's private key is stored on the secure site
- When the user touches the finger sensor the finger template passes over an encrypted link to the site to unlock the private key for signing or decryption

Why is this implementation critical?

- Exiting encryption implementations assume that the *possession* of a secret key is equivalent to a signature
- This requires that the user "own" the key and keep it totally secret: on a hard-disk, token, or smart card
- This may be thought of as the "key-under-the-mat" strategy: security by wishful thinking
- In our system the key is kept in the *most* secure place (the server) and linked to the user through their irrevocable, unique, impossible-to-lose fingerprint

What are the advantages?

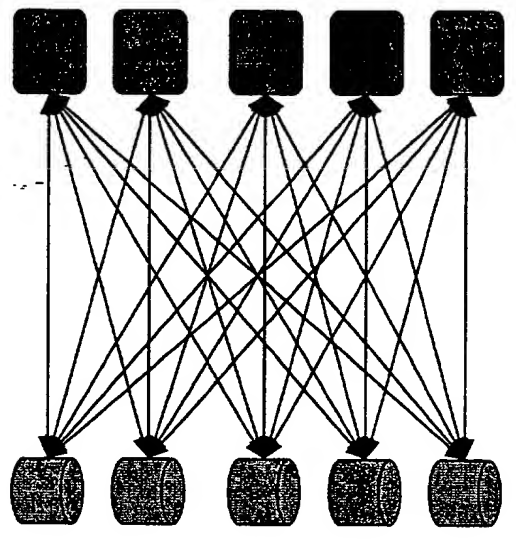
- User access is through a single, secure touch: the one action can sign, encrypt or decrypt a document
- The system is Web based - only a sensor need be attached to any browser-enabled device
- The security is open: signed and/or encrypted email and documents will be able to move both into and out of the system
- Private keys are centrally stored and managed rather than the existing client-based "key-under-the-mat" strategy that is both insecure and non-portable

The community as a portal

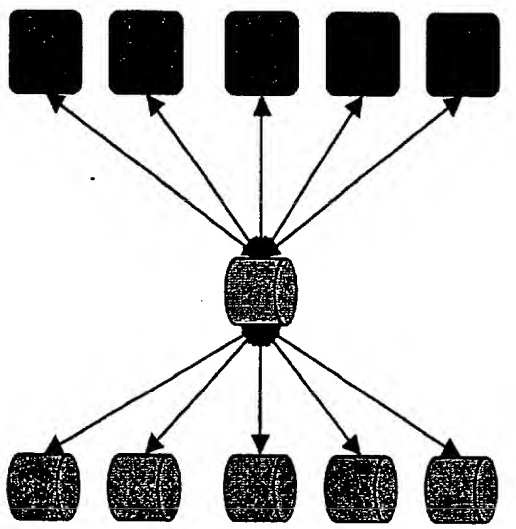
- The community has the unique ability to unambiguously identify the user
- This allows the community to carry the user to outside merchants (shops, banks, etc) with specific guarantees such as
 - ! **Identity: this is the individual John Doe**
 - ! **Payment: this person can pay up to \$200**
 - ! **Age: this person is over 18 years old**
- This allows the community to add value as a portal: guarding the privacy of members while conveying to merchants the information they need for transactions

Simplifying trust

1-to-1:
Many trust relationships



Trusted Portal:
Far fewer trust relationships



 Customers

 Merchants

 Trusted Portal

Appendix: Process flow

- Finger detected on sensor
- Fingerprint is acquired, image is transferred to client
- Template extracted from image & browser initialized
- SSL used to transmit template to server
- Template is used at server to validate user identity
- Browser session begins
- Any sign, encrypt or decrypt operation requires a new touch to release use of private key on server

Secure Site

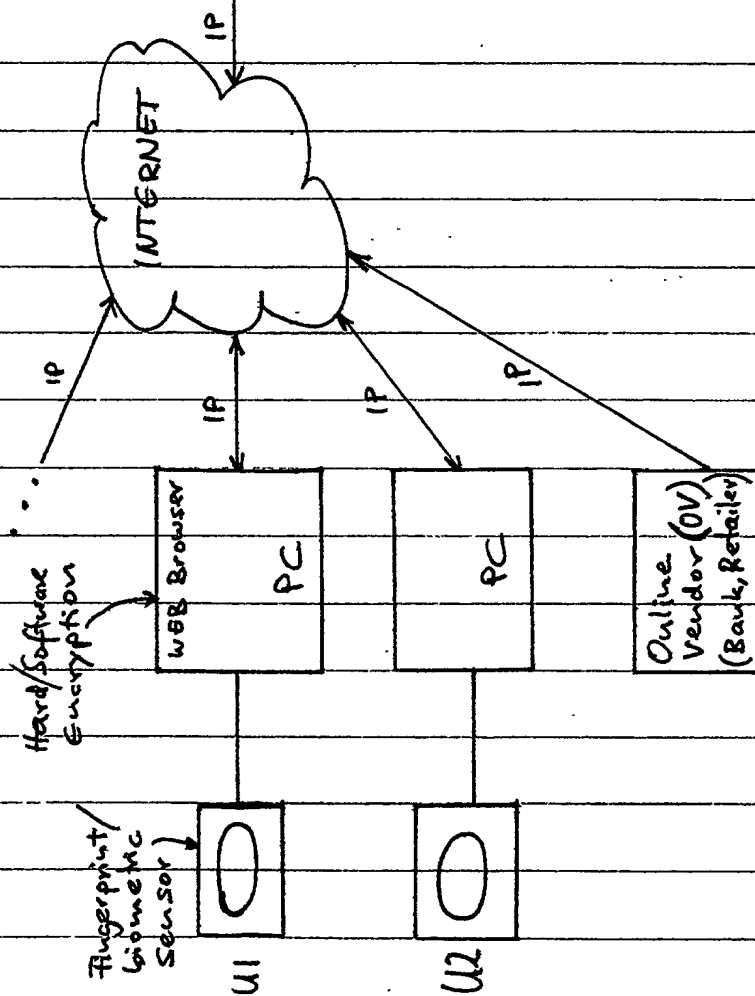
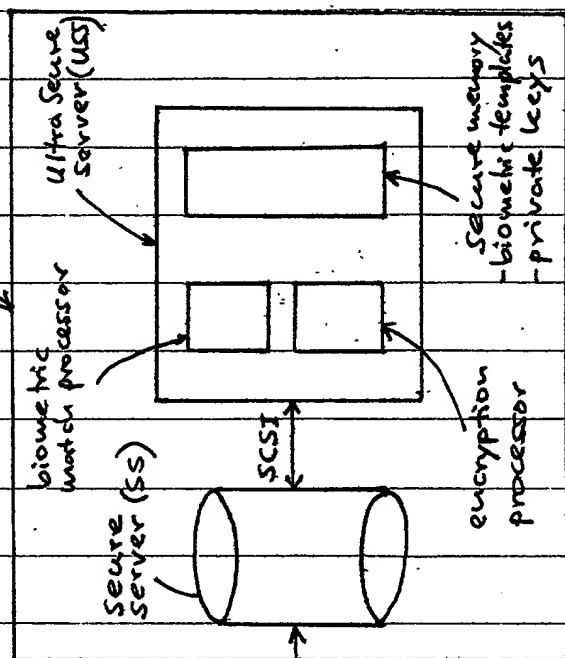


Fig. 1

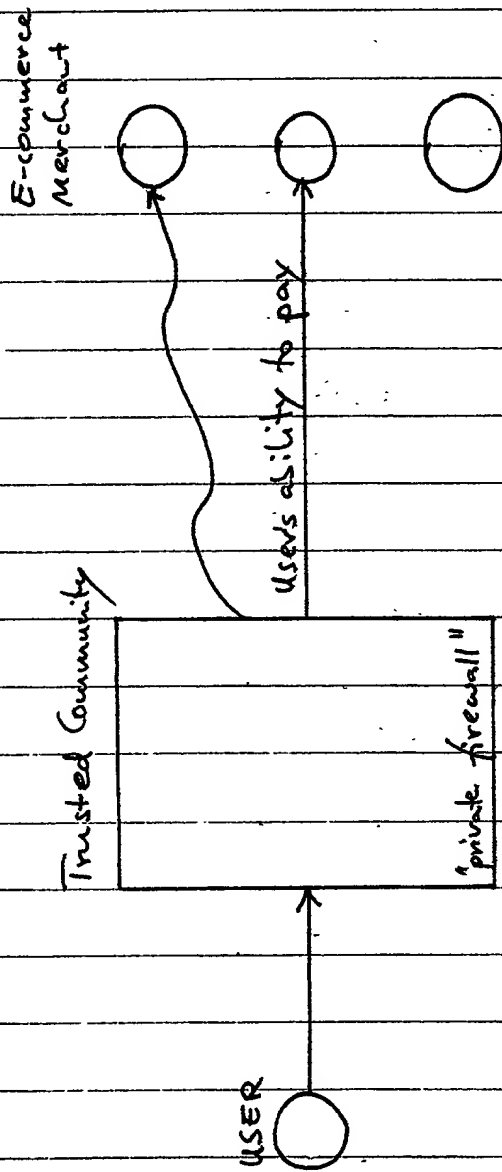


Fig. 2